International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1812

(05/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

IMT-2020 Security

Security framework based on trust relationships for the IMT-2020 ecosystem

Recommendation ITU-T X.1812

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	**X.1800–X.1819**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1812

Security framework based on trust relationships for the IMT-2020 ecosystem

Summary

Recommendation ITU-T X.1812 identifies stakeholders in an International Mobile Telecommunications-2020 (IMT-2020; also known as fifth generation) ecosystem, analyses trust relationships amongst them, identifies threats and clarifies security responsibilities for each stakeholder, specifies security boundaries between stakeholders, and establishes a security framework based on these trust relationships.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1812	2022-05-20	17	11.1002/1000/14808

Keywords

Ecosystem, framework, IMT-2020, trust.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

The set of stakeholders in an International Mobile Telecommunications-2020 (IMT-2020; also known as fifth generation (5G)) system is larger and more varied than in previous communication systems. In the second, third and fourth generation (2G, 3G and 4G), the main stakeholders can be summarized as service providers, network operators, equipment vendors and subscribers. However, in an IMT-2020 ecosystem, vertical players are also involved, such as industrial and commercial enterprises. Also, service providers can be sub-divided into cloud platform operators, data analyst companies, application providers, etc. Furthermore, at the terminal end, subscribers are not only end users as was the case previously. Subscribers can include a range of different types of stakeholder, especially for commercial terminals, e.g., in the shared vehicle communication use case. These changes create complex relationships among various stakeholders and raise a series of new security issues for IMT-2020 ecosystems.

The IMT-2020 network also introduces new features. For example, the introduction of network virtualization in IMT-2020 breaks the fixed connections between network entities and enables software-defined networks. Another example is provided by service-based architecture. With such architecture, more cloud-related features could be built into an IMT-2020 network. Also, slicing can enable more effective co-operation between an IMT-2020 network and services.

As time goes on, increasing numbers of information technology (IT) techniques will be applied to IMT-2020 systems, not only to their services, but also their network. The IMT-2020 network is entirely based on the Internet protocol. Its architecture specification is based on services rather than reference points, as was the case for previous network architectures. Signals are increasingly transferred from the Internet rather than dedicated networks. The transport protocol in IMT-2020 networks is changed from diameter [b-IETF RFC 6733], which is less popular than the hypertext transfer protocol that is widely used globally. All these changes will bring benefits for the IMT-2020 network and service deployment and operation.

However, the use of popular protocols and an open connection environment could also bring benefits to attackers. An attacker will not need to spend that much time studying complex telecommunication protocols, and it will potentially be simpler to find an intrusion point in a network. As a result, in IMT-2020 networks it is not reasonable to assume that internal communication is trustworthy anymore. Thus, the changes from 4G to IMT-2020 break the trust relationship between network operators.

Additionally, the IMT-2020 network is designed to be more flexible in order to meet the varied service requirements. In particular, slicing has been introduced into IMT-2020 networks. IMT-2020 networks can also expose some capabilities to services. Such capability exposure will enable an IMT-2020 service to control some network functions. These new features will make the security boundary between the IMT-2020 network and services more ambiguous.

This Recommendation identifies stakeholders in an IMT-2020 ecosystem, analyses trust relationships among them, identifies threats and clarifies security responsibilities for each stakeholder, specifies security boundaries between stakeholders and establishes a security framework based on these trust relationships.

Recommendation ITU-T X.1812

Security framework based on trust relationships for the IMT-2020 ecosystem

1 Scope

This Recommendation specifies a security framework based on trust relationships for an International Mobile Telecommunications-2020 (IMT-2020) ecosystem. This Recommendation describes a general approach to the:

- identification of scenarios for providing IMT-2020 services;
- identification of stakeholders in an IMT-2020 ecosystem;
- analysis of trust relationships among stakeholders;
- identification of threats applying to each stakeholder;
- clarification of security responsibilities for each stakeholder;
- specification of security boundaries between stakeholders;
- specification of security requirements based on trust model; and
- establishment of a security framework based on the trust relationships between stakeholders.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 business unit [b-ISO/TS 21089]: Discrete and accountable function or sub-function within an organization

NOTE – A business unit can include a department, service or specialty within a healthcare provider organization.

3.1.2 deployment [b-ISO/IEC/IEEE 24765]: Phase of a project in which a system is put into operation and cutover issues are resolved.

3.1.3 developer [b-NIST SP 800-53]: An entity that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers.

3.1.4 domain [b-ISO/IEC 14888-1]: Set of entities operating under a single security policy.

EXAMPLE – Public key certificates created by a single authority or by a set of authorities using the same security policy.

3.1.5 information system [b-ISO/IEC 27000]: Set of applications, services, information technology assets, or other information-handling components.

3.1.6 lifecycle [b-ISO/IEC/IEEE 15288]: Evolution of a system, product, service, project or other human-made entity, from conception through retirement.

3.1.7 network function [b-ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

NOTE 1 – Network functions include but are not limited to network node functionalities, e.g., session management, mobility management and transport functions, whose functional behaviour and interfaces are defined.

NOTE 2 – Network functions can be implemented on a dedicated hardware or as virtualized software functions.

NOTE 3 – Network functions are not regarded as resources, but rather any network functions can be instantiated using the resources.

3.1.8 stakeholder [b-ISO/PAS 19450]: Individual, organization, or group of people that has an interest in, or might be affected by the system being contemplated, developed, or deployed.

3.1.9 supplier [b-ISO 10393]: Organization or person that provides a product or service.

3.1.10 system development [b-ISO/IEC 2382]: Process that usually includes requirements analysis, system design, implementation, documentation and quality assurance.

3.1.11 trust [b-ISO/IEC 25010]: Degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

3.1.12 trust level [b-ISO 28598-1]: Customer's estimate of the weight of prior, supplementary and indirect evidence of the supplier's capability to fulfil the specified quality requirements.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 external service provider: A set of entities that includes: a) entities within the organization but outside the security authorization boundaries established for organizational information systems; b) entities outside the organization either in the public sector (e.g., federal agencies) or private sector (e.g., commercial service providers); or c) some combination of the public and private sector options.

NOTE – Adapted from [b-NIST SP 800-53].

3.2.2 supply chain: A network of organizations that are involved, through upstream and downstream linkages, in the processes and activities that produce value in the form of products and services in the hands of the ultimate consumer.

3.2.3 system development lifecycle: A structured approach to planning, creating, testing, deploying and maintaining an information system.

3.2.4 trust model: Model that consists of components that describe the trust relationships and chains between stakeholders.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G	second Generation
3G	third Generation
4G	fourth Generation
5G	fifth Generation
5GC	fifth Generation Core
BS	Base Station

CAB	Conformity Assessment Body
E2E	End to End
HO	Home Operator
ICP	Internet Content Provider
ICT	Information and Communication Technology
IMT-2020	International Mobile Telecommunications-2020
IoT	Internet of Things
IoV	Internet of Vehicles
IPX	Internetwork Packet exchange
ISP	Internet Service Provider
IT	Information Technology
NE	Network Element
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NFV	Network Function Virtualization
NPN	Non-Public Network
PII	Personally Identifiable Information
PLMN	Public Land Mobile Network
SCAS	Security Assurance Specification
SDL	Security Development Lifecycle
UICC	Universal Integrated Circuit Card
VNF	Virtualized Network Function
VO	Visited Operator

5 Conventions

In this Recommendation:

The phrase "**is recommended**" indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformity.

The phrase "**can optionally**" indicates an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformity with this Recommendation.

6 Overview

Before the 5G era, telecommunication systems were mainly used for providing telephony, Internet access and related services. As a result of the capability and rate constraints of these systems, the use cases were simple in general. In particular, only a small number of roles was involved in a communication system. For the call service, the players involved are the caller, the callee and the mobile network. For the data service, the players are the terminal, the mobile network and service or application providers. In addition, in order to support the building of networks and application systems, vendors are involved. Terminal manufacturers and universal integrated circuit card (UICC) providers are relevant at the terminal. These are the main roles involved in 2G, 3G and 4G telecommunication systems.

However, in the IMT-2020 ecosystem, things are different. The ecosystem does not only contain all stakeholders in telecommunication system in terminal, network and service, but also other stakeholders. At the terminal, subscribers are not only end users, as was the case before, because the mobile device could be one of many different types of equipment that may be shared between multiple parties, not just a telephone. In the network, IMT-2020 introduces a range of new features. For example, network virtualization in IMT-2020 breaks the fixed connection between network entities and enables software-defined networks that break the security border of network deployment. More and more information technology (IT) techniques are applied in IMT-2020 networks that can also be exploited by attackers. The network exposure service opens interfaces in the control plane rather than the user plane for an attacker. For services, vertical players are involved, such as industrial and commercial enterprises. This divides service providers into cloud platform operators, data analyst companies, application providers, etc., as shown in Figure 1.

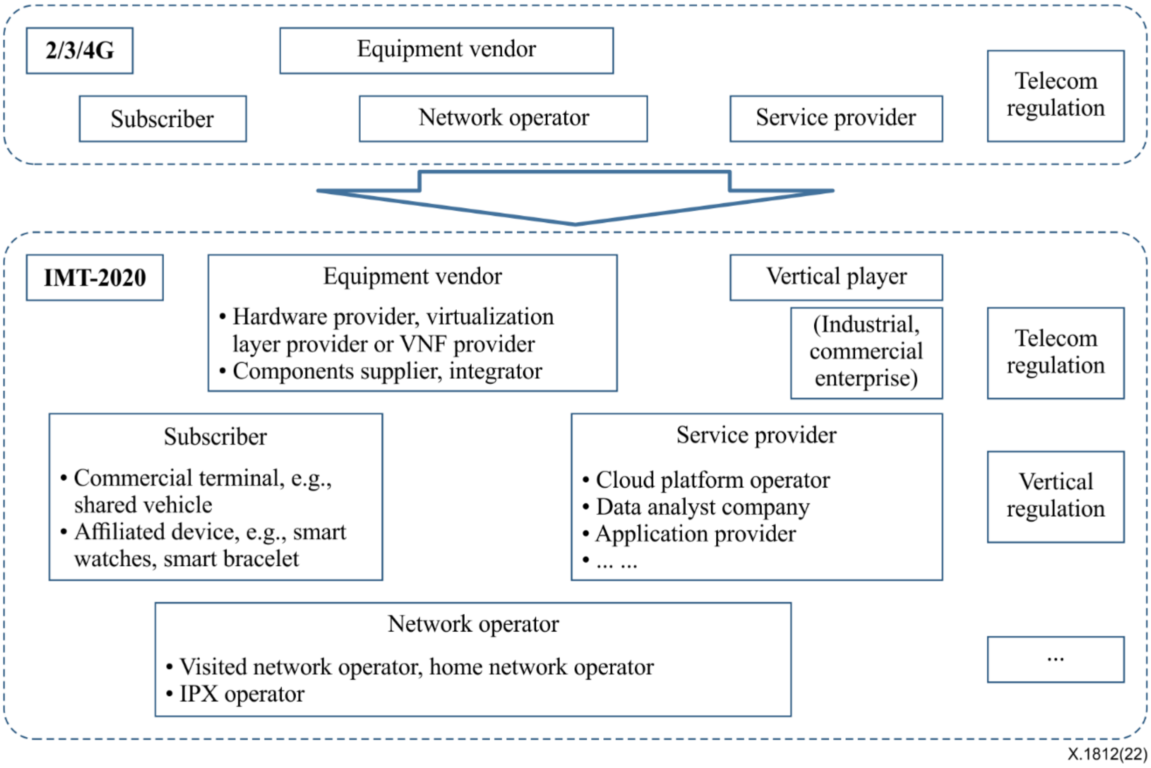

2/3/4G
Equipment vendor
Telecom regulation
Subscriber
Network operator
Service provider
IMT-2020
Equipment vendor
• Hardware provider, virtualization layer provider or VNF provider
• Components supplier, integrator
Vertical player
(Industrial, commercial enterprise)
Telecom regulation
Subscriber
• Commercial terminal, e.g., shared vehicle
• Affiliated device, e.g., smart watches, smart bracelet
Service provider
• Cloud platform operator
• Data analyst company
• Application provider
• ... ...
Vertical regulation
Network operator
• Visited network operator, home network operator
• IPX operator
...
X.1812(22)

Figure 1 – Ecosystem evolution from 2G, 3G, 4G to IMT-2020

In this case, the trust relationship of the IMT-2020 system is different. Users or subscribers and network or service systems are much closer than before. The complex and long-tailed supply chain pushes operators to consider more about the evaluation of suppliers. The tight bond between service and network makes vertical industries rely heavily on the network and requires more strict trust and security. Provision of a new trust model for the IMT-2020 ecosystem needs consideration, to formulate a clear security requirement and security boundary between stakeholders. In this way, communication efficiency can be improved as much as possible with assurance of data security.

Five properties, namely resilience, communication security, identity management, personally identifiable information (PII) protection and security assurance, impact the trustworthiness of an IMT-2020 system.

- Resilience: Resilience is the capability of an organization to resist being affected by disruptions. A variety of complementary and partially overlapping features in IMT-2020 can help achieve resilience of an IMT-2020 system to cyberattacks and non-malicious incidents.
- Communication security: Communication security is applied to data communication in IMT-2020. Secure communication for devices and for its own infrastructure is vital in an IMT-2020 system.
- Identity management: An identity management system consists of processes and policies involved in managing the lifecycle, value, type and optional metadata of attributes making up identities of entities in an IMT-2020 system. Provision of secure identity management for identification and authentication of subscribers, roaming or not, and ensuring that only genuine subscribers can access network services is recommended. Such systems are built on strong cryptographic primitives and security characteristics.
- PII protection: Data privacy is defined in [b-ISO/TS 21719-2] as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information. PII protection involves protecting PII that can be used by unauthorized parties to identify subscribers.
- Security assurance: Security assurance provides grounds for justified confidence that a claim about meeting security objectives has been or will be achieved. Security assurance is a means to ensure that network equipment meets security requirements and is achieved through the adoption of secure development and product lifecycle processes.

7 Security framework supported by the trusted model

This Recommendation analyses and determines the roles of stakeholders in the IMT-2020 ecosystem and the trust relationship between roles by analysing several typical scenarios. It then tries to determine the level of trust with the key factors to be considered. On this basis, it gives recommendations on how to determine security requirements based on the trust level, and to form a security framework based on trust relationship, as shown in Figure 2.

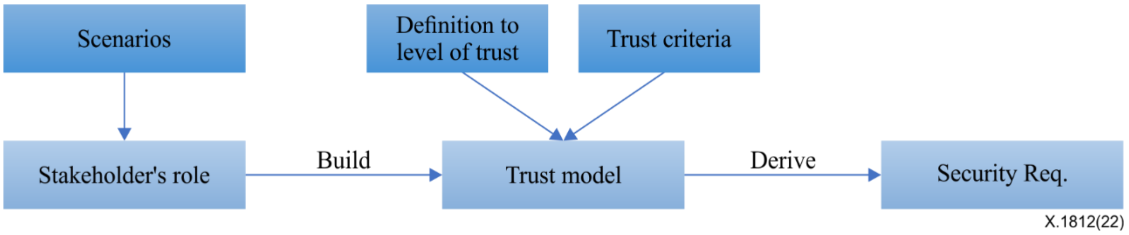


Figure 2 – Way forward to build security framework based on trust relationships for IMT-2020 ecosystem

Based on the role and relationship, trust model and security requirements of all stakeholders, a security framework supported by the trust model established in this Recommendation is illustrated in Figure 3. All components in the framework are described in: clause 8 for the stakeholders' role; clause 9 for the trust model; and clause 10 for security requirements.

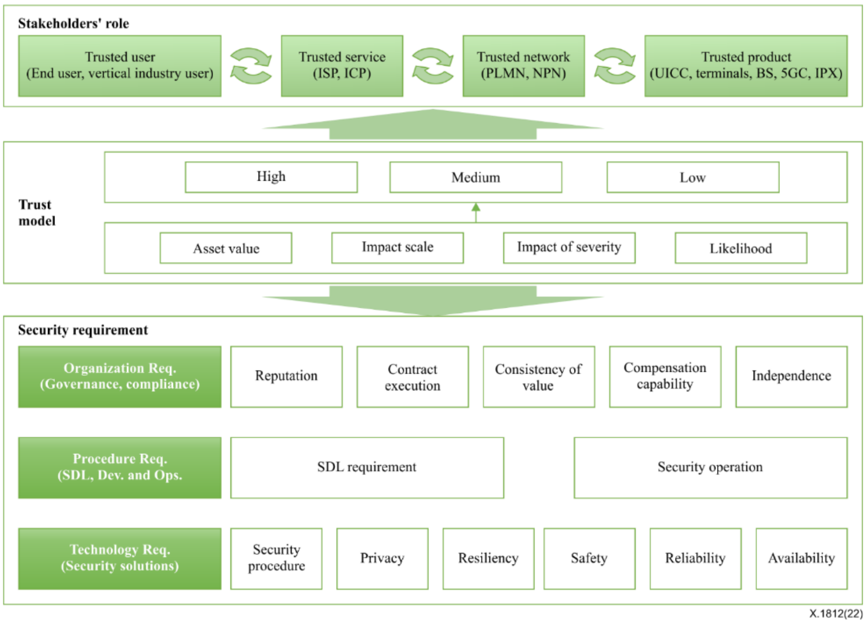


Figure 3 – Security framework supported by the trusted model based on trust relationship between stakeholders

5GC: fifth generation core; BS: base station; ICP: Internet content provider; ISP: Internet service provider; NPN: non-public network; SDL: security development lifecycle

8 Stakeholder role in scenarios for the IMT-2020 ecosystem

8.1 General

The current telecommunication system can be subdivided into three sub-systems: terminal; network; and service. It is necessary to consider the possible relationships both between each sub-system and within a sub-system. As the terminal-network relationship has already been studied by other standard organizations such as the 3rd Generation Partnership Project (3GPP), it is not further addressed in this clause.

Collectively, the set of five scenarios addressed in this clause covers all possible intersystem relationships except for the terminal-network relationship.

8.2 Scenario 1: Virtualization network deployment in a network operator domain

8.2.1 General

This scenario focuses primarily on the inner-network relationship.

In current telecommunication networks, network elements (NEs) that are deployed in a network are usually implemented as dedicated physical devices. Each NE is implemented as one or more physical entity servers, based on its capability. Cables, fibres, switches and routers are used to connect such network devices through physical interfaces. In this scenario, the main stakeholders are: users or subscribers; mobile terminal manufacturers; UICC providers; network device vendors; and operators. This is shown in Figure 4.

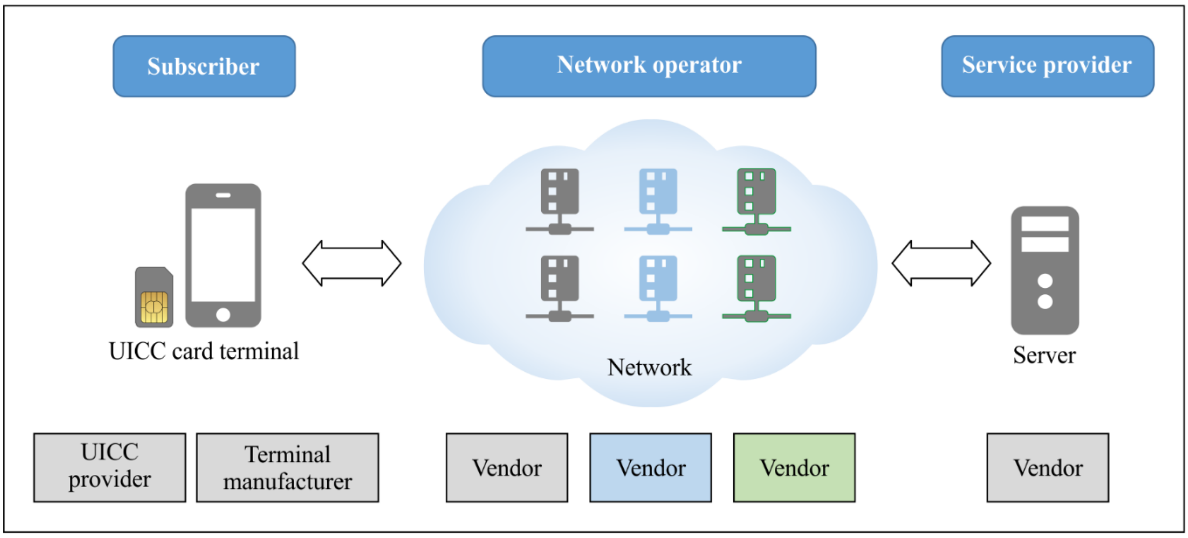


Figure 4 – Main stakeholders in a network operator domain

In IMT-2020, software-defined networking/network function virtualization) technology has been significantly developed, and has gradually begun to be deployed in the network. Telecommunication networks are also developing with increasing use of IT. When the IMT-2020 network architecture was designed, a novel service-based architecture was introduced to make better use of IT for deployment and maintenance. The NE is replaced by the network function (NF), which is more flexible to operate and maintain. The NF can be implemented as a virtualized network function (VNF), and even in the form of software applications running on a virtual machine. This suggests that network virtualization will be widely used in the deployment of IMT-2020 networks. In this way, implementation has changed from the original hardware- and software-integrated devices to a three-layer combination of hardware, virtual layer and VNF. As a result, the main stakeholders involved in this scenario are: users or subscribers; mobile terminal manufacturers; UICC providers; NEs vendor (hardware providers, virtualization layer providers, VNF providers); and network operators. This is summarized in Figure 5.

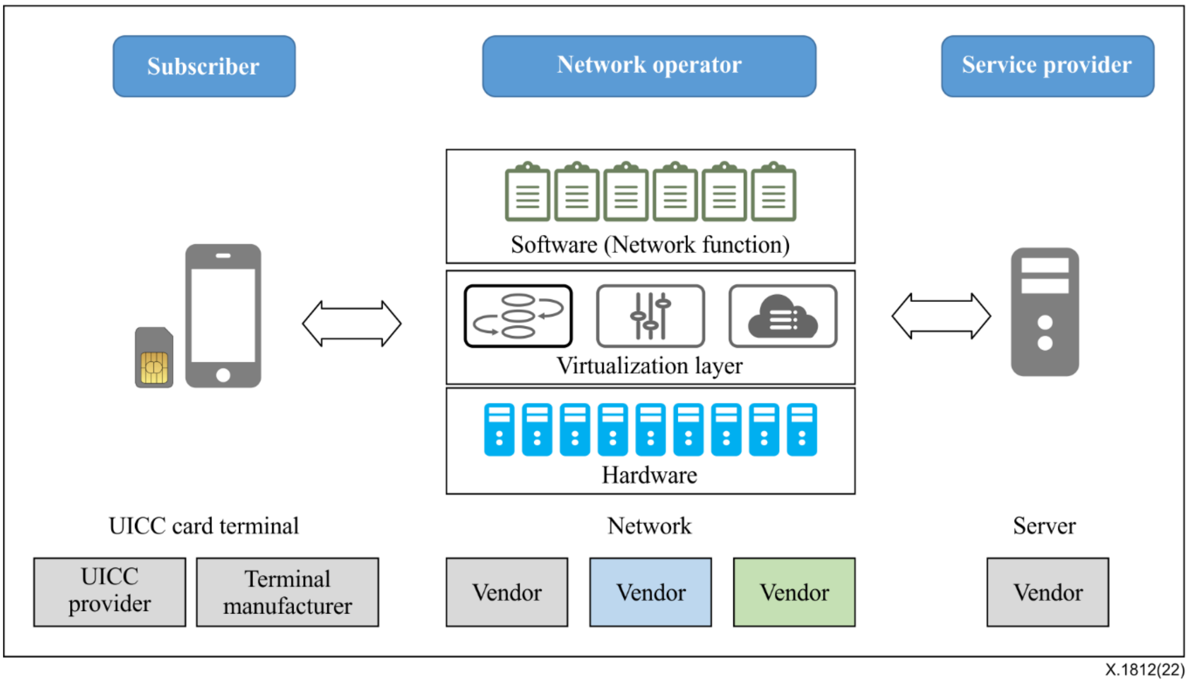


Figure 5 – Main stakeholders in virtualization network deployment of a network operator domain

8.2.2 Roles of stakeholders in this scenario

These stakeholders take the following roles in this scenario.

- Users or subscribers: These are the ultimate users, i.e., customers, of the telecommunication services. The subscriber equipment consists of the mobile terminal provided by a manufacturer and a UICC provided by a card vendor.
- Mobile terminal manufacturer: This entity provides terminals that can be used by users or subscribers communicating with a network.
- UICC provider: This entity provides UICCs that can be used to represent subscriber identities.
- NE vendor: This entity offers devices or components in devices that can be composed to create the telecommunication system or service platform/system.

  NOTE – If providing components, it can be further categorized into one of hardware provider, virtualization layer provider or VNF provider.
- Network operator: This entity owns or controls all the elements necessary to sell and deliver telecommunication services to subscribers and service providers.

8.3 Scenario 2: Interconnection and roaming

8.3.1 General

This scenario focuses primarily on the inner-network relationship.

The mobile telecommunications network can provide services for worldwide users based on interconnection and coordination between global operators. Such interconnection and coordination between operators involve coordination and cooperation in the service and transport layers.

Until now, the design principle for interconnection between public land mobile network (PLMN) operators assumed that operators (at the service level) could completely trust each other, and the transmission of signalling and user data could also be trusted. In order to ensure forwarding of signalling messages to a specific operator correctly, the internetwork packet exchange (IPX) provider was introduced. However, with network growth and the use of the Internet, IPX connections have become increasingly complex, and can also be attacked via the Internet. As a result, operators can only guarantee security for IPX connections directly connected to them, and not for links between operators and all other links of operators. This is shown in Figure 6.

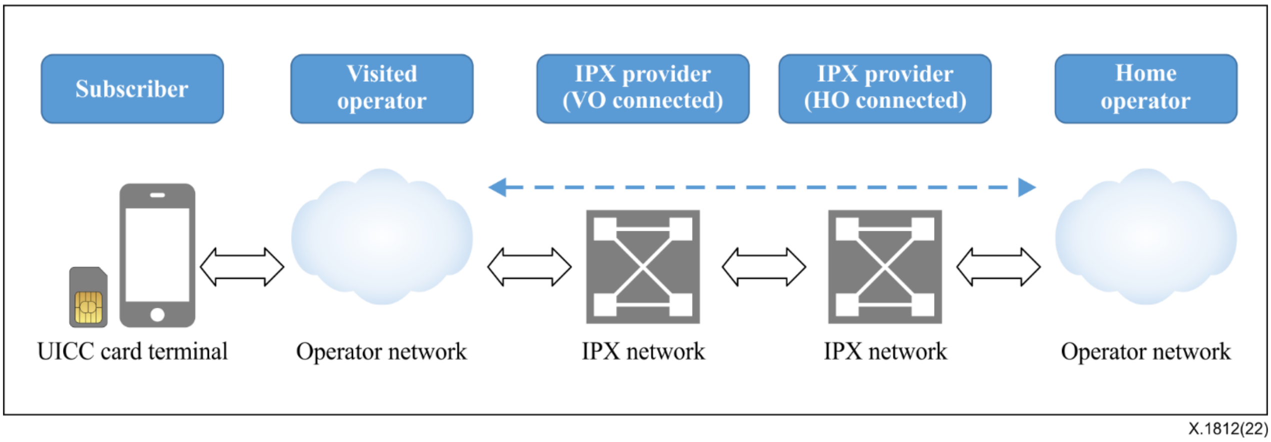


Figure 6 – Main stakeholders in interconnection and roaming scenario

HO: home operator; VO: visited operator

Also, many vulnerabilities in operators have been found and exploited, allowing attackers to launch attacks on other operators by using compromised devices as a springboard. As a result, messages in the services layer are also no longer trusted by operators [b-3GPP TS 33.501].

In such a scenario, the main players involved are users or subscribers, visited operators, home operators and IPX operators (including IPX-connecting visited operator and IPX-connecting home operator).

8.3.2 Roles of stakeholders in this scenario

These stakeholders take the following roles in this scenario.

- User or subscriber: This is the ultimate user, i.e., customer, of telecommunication services.
- Visited operators: Such operators provide access services to the subscriber when the subscriber is outside the coverage of its home network operator.
- Home operator: This operator owns subscriber subscriptions and provides services to them.
- IPX operator (IPX-connecting visited operators, or IPX-connecting home operator): This entity provides an internetworking packet exchange service between operators.

8.4 Scenario 3: Car rental with remote operation

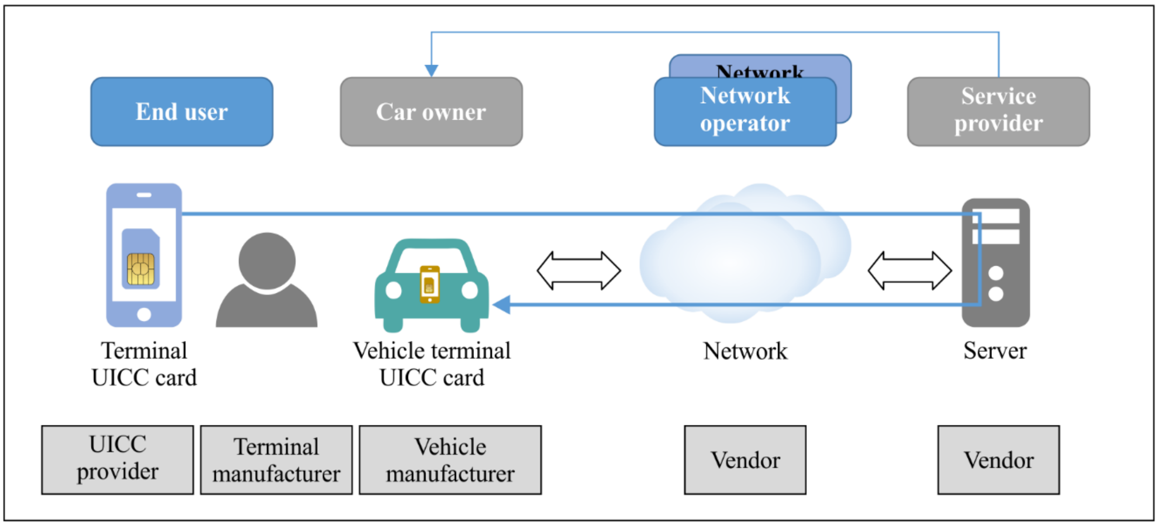
8.4.1 General

This scenario focuses primarily on inner-terminal relationship and terminal-service relationship.

There are more and more vehicles that communicate with the remote platform by using a built-in or post-installed communication module. Such vehicles can upload specific status to or get instructions from a remote platform. In this situation, the vehicle is constructed of two parts: one related to telecommunication, which is provided by the terminal manufacturer; and the other is the vehicle itself, which is made in vehicle factory.

The traditional mobile communication network mainly provides voice, short message or data network access services to subscribers. The subscriber is the end user of the terminal. For car rental services, the drivers who use vehicles containing communication terminals are not subscribers. In another aspect, car renters usually need to use an application on their mobile terminal to interact with the platform through a communication network, in order to get vehicle information remotely or operating a rented vehicle remotely, such as locating the vehicle, unlocking or closing the door without keys, or starting or shutting down the air conditioning.

Therefore, in such a case, as shown in Figure 7, the main stakeholders involved are car renters, the vehicle (which is a mobile terminal), mobile terminal manufacturers, UICC providers, automobile manufacturers, NE vendors, network operators and application providers.



X.1812(22)

Figure 7 – Main stakeholders in car rental with remote operation scenario

8.4.2 Roles of stakeholders in this scenario

These stakeholders take the following roles in this scenario.

- Car renter: A specific user rents a car from a car hire firm. This person is also a subscriber to a mobile network with a mobile terminal.
- Vehicle: Vehicle belongs to a car hire firm with an embedded specific mobile terminal that can be seen as a network subscriber.
- Mobile terminal manufacturer: The entity provides terminals that can be used by subscribers communicating with the network.
- UICC provider: The entity provides UICCs that can be used to represent subscriber identities.
- Automobile manufacturer: The entity produces vehicles that may or may not contain a mobile terminal.
- NE vendor: The entity offers devices or components of devices that can be composed for telecommunication system or service platform or system.
- Network operator: The entity owns or controls all the elements necessary to sell and deliver telecommunication services to subscribers and service providers.
- Application provider: The entity provides applications for car rental service for users.

8.5 Scenario 4: Network capability exposure for industry

8.5.1 General

This scenario is mainly focused on the network-service relationship and inner-service relationship.

IMT-2020 owns new features such as enhanced mobile broadband, massive Internet of things (IoT) connection and ultra-reliable low-latency communication. With these features, an IMT-2020 network can provide better network connection support for vertical areas such as industry.

Compared to personal communication, vertical industry communication needs are different, such as service diversity, functional differentiation and technology heterogeneity. Vertical communication in the application layer usually has strict security requirements, such as communication isolation from other industry users, more management ability or collaboration with network operators with specific features such as capability exposure.

Compared with traditional services, vertical industry services may cooperate with network operators, so application providers are introduced, and providers related to the application server or cloud platform are also involved.

On the terminal side, like scenario 3, the terminal device may also contain two parts, one related to communication, provided by the terminal manufacturer, the other is related to dedicated vertical applications, provided by other industrial terminal manufacturers.

In such a case, as shown in Figure 8, the main stakeholders involved are: vertical industry users; communication terminal manufacturers; UICC providers; industrial terminal manufacturers; NE vendors; application server providers or cloud platform service providers; application providers; and network operators.

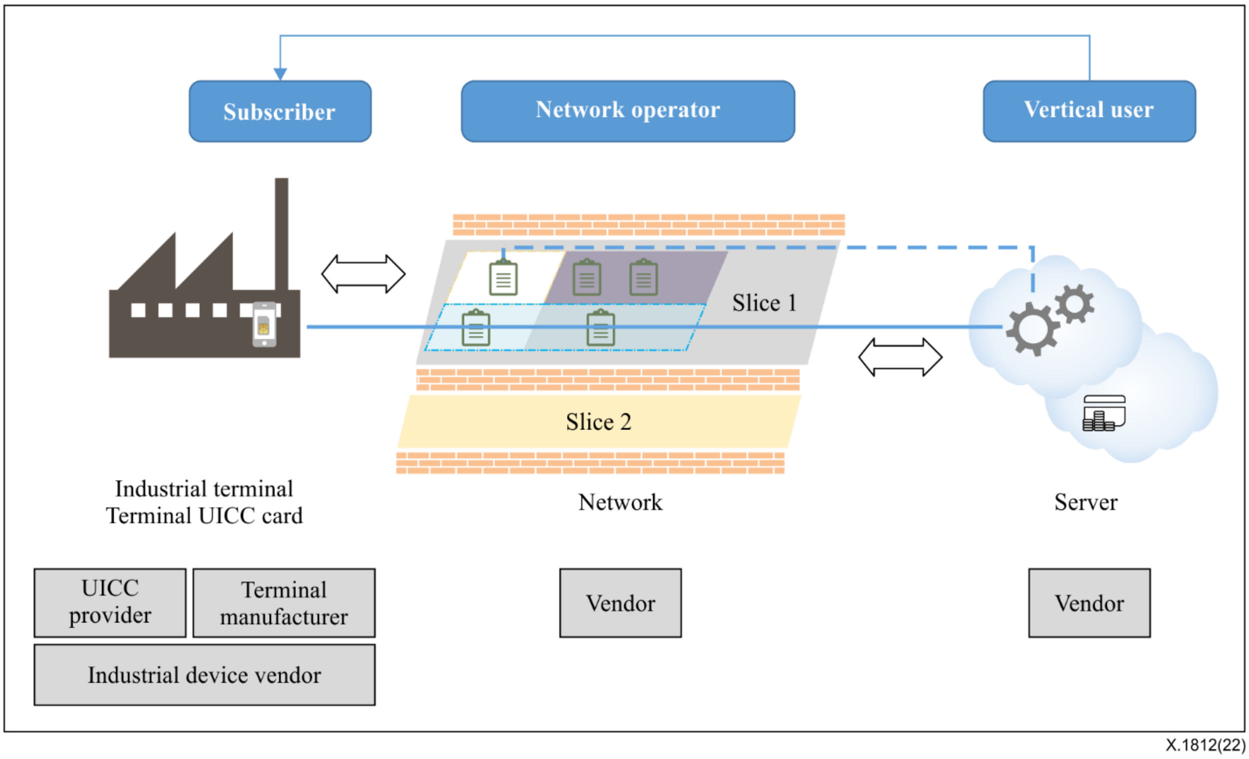


Figure 8 – Main stakeholders in network capability exposure scenario

8.5.2 Roles of stakeholders in this scenario

The main stakeholders take the following roles in this scenario.

- Vertical industry user: Vertical industry user controls an industrial terminal remotely through the telecommunication network, by using dedicated applications running on application servers or public or private cloud platforms.
- Communication terminal manufacturer: The entity provides terminals that can be used by subscribers communicating with the network.
- UICC provider: The entity provides UICCs that can be used to represent subscriber identities.
- Industrial terminal manufacturer: The entity delivers an industrial machine, network or system for a factory or enterprises.
- NE vendor: The entity offers devices or components of devices that can be composed for telecommunication system or a service platform or /system.
- Application server provider or cloud platform service provider: The entity owns the infrastructure and platform that offer storage and computing resource services for upper layer applications.

- Application provider: The factory or enterprises gather information or provide control signalling to industrial terminals.
- Network operator: The entity owns or controls all elements necessary to sell and deliver telecommunication services to subscribers and service providers.

8.6 Scenario 5: Supply chains

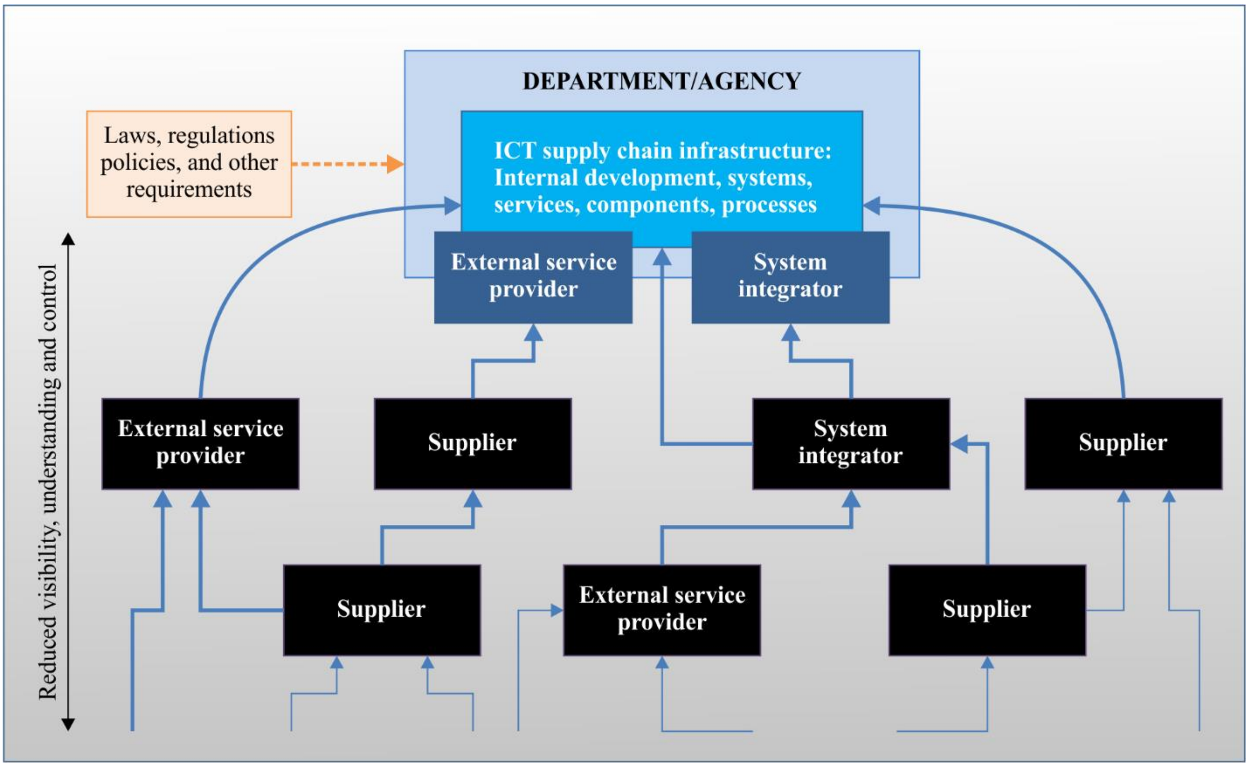
8.6.1 General

The IMT-2020 ecosystem refers to a community comprising many organizations contributing vast amounts of technologies and expertise to make IMT-2020 services and applications work.

A supply chain is a system of organizations, people, activities, information and resources involved in moving a product or service from supplier to customer. Supply chain risk management is the coordinated efforts of an organization to identify, monitor, detect and mitigate threats to supply chain continuity and profitability. There are four security pillars for supply chain risk management for IMT-2020 ecosystem as follows.

- Security aspect: This deals with the confidentiality, integrity and availability of information that: a) describes the supply chain (e.g., information about the transversal paths of IMT-2020 products and services, both logical and physical); or b) traverses the supply chain (e.g., intellectual property contained in IMT-2020 products and services), as well as information about the stakeholders participating in the supply chain (anyone who touches an IMT-2020 product or service throughout its lifecycle);
- Integrity aspect: This ensures that IMT-2020 products or services in the supply chain are genuine and unaltered, and that the products and services will perform according to acquirer specifications and without additional unwanted functionality.
- Resilience aspect: This ensures that the supply chain provides the required products and services in the case of stress and failure;
- Quality aspect: This reduces vulnerabilities that may limit the intended function of a component, lead to component failure or provide opportunities for exploitation.

This scenario is mainly focused on supply chains and relationships. Figure 9 illustrates the main players in supply chain scenarios**.**


DEPARTMENT/AGENCY
Laws, regulations policies, and other requirements
ICT supply chain infrastructure: Internal development, systems, services, components, processes
External service provider
System integrator
Reduced visibility, understanding and control
External service provider
Supplier
System integrator
Supplier
Supplier
External service provider
Supplier
X.1812(22)

ICT: information and communications technology

Figure 9 – Main stakeholders in supply chain scenarios

8.6.2 Roles of stakeholders in this scenario

There are several stakeholders for a supply chain: developer or manufacturer; system integrator; vendor; product resellers; supplier; and external service provider.

The developer or manufacturer refers to: i) developers or manufacturers of information systems, system components or information system services; ii) systems integrators; iii) vendors; or iv) product resellers.

A system integrator is a person or company that deals with bringing together component sub-systems into a whole and ensuring that those sub-systems function together, a practice known as system integration.

A vendor is anyone who provides goods or services to a company or individuals. A vendor often manufactures items and then sells them to a customer. An enterprise is a separate legal entity from the contracting company that provides services such as consulting or software development.

A product reseller is a company or individual that purchases goods or services with the intention of selling them rather than consuming or using them.

A supplier is an entity that supplies goods and services to another.

The external service provider refers to: i) entities within the organization but outside of the security authorization boundaries established for organizational information systems; ii) entities outside of the organization either in the public sector (e.g., federal agencies) or private sector (e.g., commercial service providers); or iii) some combination of the public and private sector options.

8.7 Stakeholders in the IMT-2020 ecosystem

Based on the use cases described in clauses 8.2 to 8.6, the IMT-2020 ecosystem can be categorized into four kinds of stakeholders in Figure 10: manufacturer; network operator; service provider; and end user.

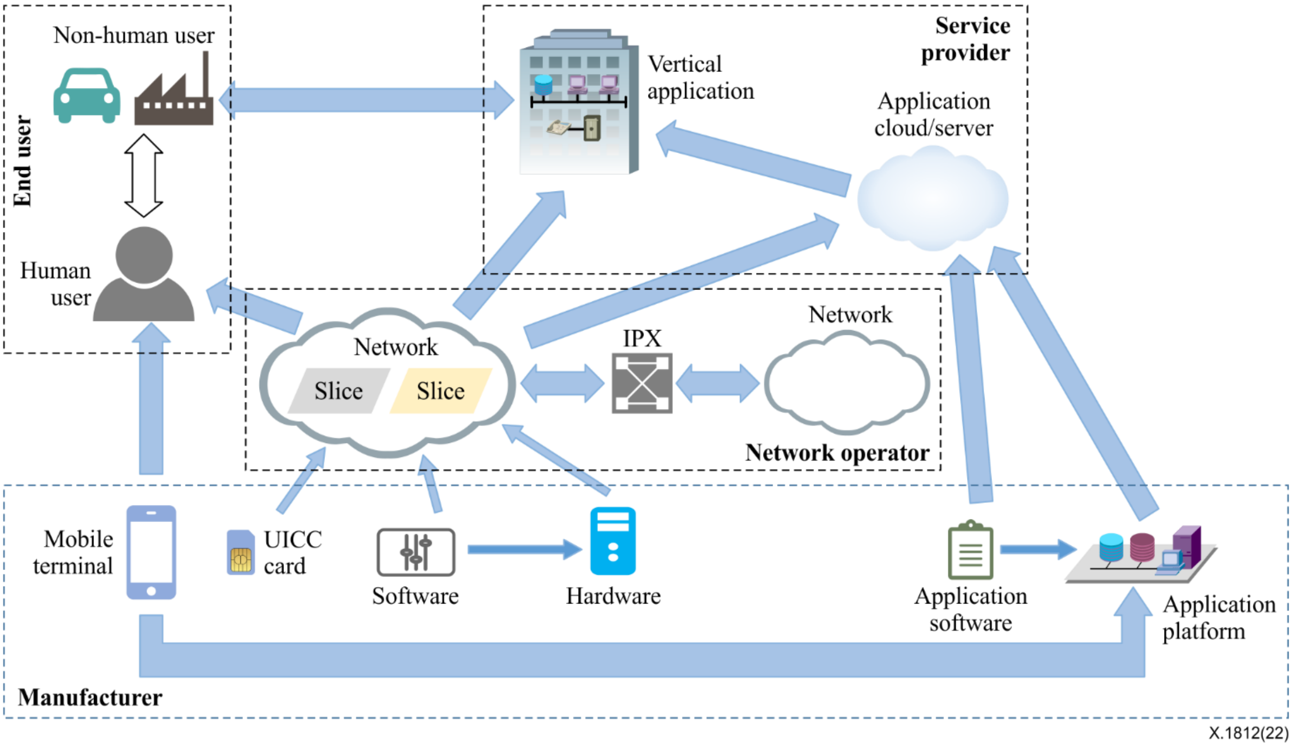


Figure 10 – Stakeholders in the IMT-2020 ecosystem

One stakeholder may have a direct relationship with another and indirect relationships with others through a stakeholder, e.g., behaving like part of a supply chain.

For the IMT-2020 ecosystem, the manufacturer can be seen as a group of developers or manufacturers, system integrators and vendors. Network operators can be seen as product resellers and network service suppliers. Service providers can be seen as external.

Component manufacturers provide technological building blocks for wireless device manufacturers and network equipment manufacturers. Such component manufacturers can also provide such building blocks directly to network operators. Wireless device manufacturers provide equipment for end users or as components of industrial machines, while network equipment manufacturers produce equipment to support network infrastructure (includes wireless and wireline). Network operators combine these devices, network components, network equipment and networks from other operators through IPX into a worldwide operational network to serve end users. End users make voice calls, send text messages and run applications over the network. Network operators also provide communication and related services for external service providers, through its network capability exposure service or other specific services.

9 Trust level, trust criteria, and trust model

9.1 General

As defined in clause 3.1.11, trust is the degree to which a user or other stakeholder has confidence that a product or system will behave as intended. Trust also plays an important role in the IMT-2020 ecosystem. This Recommendation specifies an IMT-2020 ecosystem trust model to enable stakeholders to make reasoned decisions about trust and security.

This IMT-2020 ecosystem trust model is divided into three levels.

- The first level trust is to cover trust requirements from governments and regulatory bodies. Key factors governing trust include international standard adoption, and public and transparent certification.

- The second level trust is to address trust requirements from industry organizations. Key factors for such bodies include the definition of the stakeholders, the end-to-end (E2E) solution owner, the final market user, the business model, the trust levels and the trust relationships.
- The third level trust is to secure trust by providing technical solutions based on key factors from the first and second levels.

This Recommendation focuses on the second and third levels, i.e., industry organizations and technical solutions.

The IMT-2020 network operator needs to rely on devices or equipment provided by manufacturers to establish its network system. Thus, it needs to trust manufacturers to provide devices that can meet the requirements of the network operator.

The service provider relies on the network to transmit information, so it needs to trust the network operator to ensure the data is transferred correctly in a timely manner. The service provider also needs to rely on the devices provided by manufacturers to establish its services, and thus it also needs to trust manufacturers to provide devices that can meet the requirements of the service provider.

End users need to rely on network transmission and service applications, so they need to trust that the network access provided by the network operator is legal and effective. Their trust requirements for the service provider are similar.

9.2 Trust levels

It is inherently difficult to quantify trust in a meaningful way. In the trust model established in this Recommendation, a qualitative notion of trust level is introduced to enable reasoning about the implications of different degrees of trust.

IMT-2020-enabled services operate in a range of contexts and thus have differing trust requirements. For example, different verticals carry different services and operate in different scenarios, and thus have different trust positioning. Furthermore, some industries are classified as being part of the national critical infrastructure, such as the smart grid, whereas others only operate in less critical everyday scenarios, such as car rental.

If a particular vertical is deemed to be part of the critical infrastructure, then obviously this industry will need a higher level of confidence that the IMT-2020 system will behave as intended. In other words, a higher level of trust needs to be set for this industry, as any damage will affect national stability. On the other hand, a lower level of trust would be needed for those industries where the effects of a failure have a relatively minor impact.

For example, narrow-band IoT services such as the Internet of vehicles (IoV), industrial Internet, smart grid and watering of flowers each have different trust levels, as damage to these industries have differing impacts on society or users.

The trust level for a specific use case mainly depends on the level of impact that damage to the particular vertical has on society and the nation. This is probably best determined by the vertical organization, as it will have representatives from multiple fields and the professional expertise to perform the necessary analysis; it is also part of their due diligence to specify the trust level. So, for higher trust level use-cases, the responsibility borne by the involved stakeholders is to be higher; in other words, a higher trust level also needs to be set for these stakeholders.

For the purposes of the trust model established here, it is assumed that the trust level for the various parties can be set to one of three qualitative levels: high, medium or low. This assumption is made for two main reasons:

- first, assigning quantitative values to trust levels is likely to be highly problematic, as there is no obvious metric for trust (unlike, for example, risk analysis, where the metric can be based on a combination of probability of occurrence and an assessment of annualized impact cost);

- second, this three-level scale is sufficiently rich to cover many existing use cases, and is also adopted elsewhere e.g., network equipment security assurance scheme (NESAS) [b-GSMA FS.13], [b-GSMA FS.14], [b-GSMA FS.15], [b-GSMA FS.16] for measuring trust requirements.

The problem remains of determining the meaning of these three trust levels, so that the model established in this Recommendation can be used consistently. Trust criteria, designed to enable a determination of the trust levels, are given in clause 9.3.

Given the diversity of assets and the wide range of deployment scenarios in specific verticals, in practice the general trust level needs to be further refined depending on the context. For example, the level of trust required for autonomous driving obviously varies depending on the specific IoV, campus or macro network.

The following example further illustrates the need for a complex, context-specific, trust level definition. Suppose an operator chooses network equipment manufacturers according to the specified trust level. If only one level is specified, all network equipment manufacturers need to be chosen according to a single trust level. However, the core network is more sensitive, valuable and influential than, for example, the antennas, so in a typical scenario the trust level for the core network manufacturer will need to be higher than for the antenna manufacturer.

As a further refinement, the trust level is specified separately for the business unit and the business scenario. For a vertical industry, this means separate specifications of the trust level for the whole vertical industry, and the particular vertical industry scenario. Possible combinations of trust levels for the two cases are shown in Table 1.

Table 1 – Trust level of business unit and business scenarios and relationship

Trust level of business unit	Trust level of business scenarios
High	High
	Medium
	Low
Medium	Medium
	Low
Low	Low

In order to make level specification more practical and more universal, it is recommended that the component trust level be defined in a flexible way. For example, the component trust level could be defined depending on the asset value or the deployment area.

To consider a specific example, the trust level for the whole smart grid is high, but, within the grid, the cables and electric poles are not as valuable as the sensors and signal transmission infrastructure of the IMT-2020 network. Even for the sensors and signal transmission infrastructure, a smart grid network deployed in a small city is not as sensitive as a grid network deployed in a metropolis.

Possible trust levels for relationships between a vertical industry and a stakeholder are described in Table 2.

Table 2 – Possible trust levels between a vertical industry and a stakeholder

Trust level of system	Trust level of component	Trust level of stakeholder
High	High	High
	Medium	Medium
	Low	Low
Medium	Medium	Medium
	Low	Low
Low	Low	Low

9.3 Trust criteria

Evaluating the trust level as high, medium or low requires evaluation of the trust relationships between stakeholders. The trust relationship between any two stakeholders is affected by many factors, and the trust degree between different stakeholders in one category and different stakeholders in another category will also differ. The criteria for evaluation therefore need to be specified individually.

Because the trust level is chosen to minimize harm from potential threats and the risks they cause, criteria can involve asset value, impact scale, impact severity and risk occurrence likelihood, based on risk management standards such as [b-NIST SP800-30], [b-ISO 31000] and [b-ISO/IEC 27005].

- Assets: The importance of this factor is clear. The more important an asset is, the greater the need to keep the asset under the full control of the stakeholder, and the higher the necessary trust level.
- Impact scale: For a large-scale stakeholder, the larger the scope, the greater will be the impact of any failure. Therefore, a high trust level is required if the scope of influence is large. For example, an operator will need a lower level of trust in a vendor that sells small cells covering tiny areas than in a vendor that sells core NEs covering a vast area.
- Impact severity: For a stakeholder acting as part of a key infrastructure, the consequences of damage are more serious, and hence greater effort is required to prevent such damage. This leads to a greater need for careful evaluations when interacting with other parties. Thus, the more serious the impact of a failure in a relationship, the higher the necessary trust level.
- Risk occurrence likelihood: If the occurrence likelihood is higher, the risk is more likely to occur.

The IMT-2020 ecosystem is very complex. For the various classes of stakeholders, e.g., end users, equipment manufacturers, network operators and service providers, each category contains a variety of specific instances. As confidence is a subjective concept, trust is difficult to measure and standardize, and the level of trust between two instances is also distinct. However, it is necessary to define a set of general trust levels that covers most situations, in order to provide guidance for each entity in an IMT-2020 ecosystem, namely: low, medium and high.

Table 3 provides an example of how an overall trust level can be determined based on the various trust criteria.

Table 3 – Trust level criteria

Overall trust level	Trust level criteria			
	Asset value	Impact scale	Impact severity	Risk occurrence likelihood
High	High	High	High	High
Medium	Medium	Medium	Medium	Medium
Low	Low	Low	Low	Low

When using the mapping in Table 3 it is important that the trust criteria risk level take into account risk mitigations either already in place or that will be implemented. For example, where the existing Internet is used for high-value, high-value e-commerce, the asset value, impact scale and impact severity can all be assessed as very high; moreover, superficially it would seem that the likelihood of attack will also be very high, given that the Internet communications protocols do not incorporate robust security features. Using Table 3, this would suggest that the trust level in the Internet needs to be high in order to meet the needs of e-commerce. However, despite the fact that the real-world trust level in the Internet is actually low, given that the Internet does not offer guarantees about the confidentiality, integrity or availability of communication channels, e-commerce is very widely and successfully used for huge volumes of transactions.

In fact, the reason this scenario works is that risks to confidentiality and integrity of data transfers are addressed by the routine use of transport layer security [b-IETF RFC 5246] to protect communications between the communication endpoints, which could be considered as part of the security requirements specified in clause 10.2.

In conclusion, the calculation of the required trust level is required to take account of the actual level of threat after application-specific risk mitigations have been applied. If not, unrealistic demands may be made on the level of trust required in providers of equipment and services, leading to significantly increased costs.

9.4 Trust model based on trust relationship mapping

In order to establish IMT-2020 security boundary and security measures in an interoperable standardized way, it is necessary to develop and utilize the trust model appropriately. In order to make the trust model effective, the trust relationships require analysis.

Given the factors identified in clause 9.2, the overall trust relationship between two parties is also unidirectional rather than bidirectional. An example of the analysis of trust relationships between various classes of stakeholder is shown in Table 4.

Table 4 – Trust relationships between stakeholders

Subject	**Object**			
	End user	**Manufacturer**	**Network operator**	**Service provider**
End user		Medium/low	High/medium/low	High/medium/low
Manufacturer	–		High	High
Network operator	Low	High/medium/low		High/medium/low
Service provider	High/medium/low	High/medium/low	High/medium/low	

The trust relationships among the various partners in an IMT-2020 ecosystem are typically very complex. Therefore, it is necessary to establish a trust model that can reflect this complexity. That is, the overall trust relationship can be refined to give sub-system-level trust values. An example of an analysis of trust relationships at a sub-system level is given in Table 5.

Table 5 – Sub-system-level trust relationship inside manufacturer

Subject	**Object**			
	Chipset/modem	**Module**	**Device provider**	**Software provider**
Chipset/modem		–	–	–
Module	High/medium		–	–
Device provider	High/medium	High/medium		–
Software provider	High/medium	High/medium	High/medium	

Using the model in Table 6, a car rental scenario is provided as an E2E example.

Table 6 – Trust model based on trust relationships in a car rental scenario

Subject		Object						
				Manufacturer				
		Service provider (vehicle)	Renter	Terminal /UICC	Automobile (exclude terminal and UICC)	Network equipment	Network operator	Service provider
Vehicle			Medium/low	Medium	High/medium	–	High/medium/low	High
Renter		High/medium		Medium/low	Medium/low	–	High/medium/low	High/medium/low
Manu-facturer	Terminal /UICC	–	–		–	–	High	High
	Automobile	–	–	–		–	–	High
	Network equipment	–	–	–	–		High	–
Network operator		Low	Low	High/medium/low	–	High/medium/low		High/medium/low
Service provider		High	Medium /low	High/medium/low	High/medium	–	High/medium/low	

10 Security requirements supported by trust model based on trust relationships

10.1 General

In a specific scenario, a system is established by a range of stakeholders, which provide different services and functions to ensure the system behaves and works as intended, bringing benefits to the stakeholders. These stakeholders together form the ecosystem.

During operation of the ecosystem, potential threats and dangers may arise to block business operation. To prevent the threats from causing harm, all stakeholders need to help guarantee that the ecosystem run continuously by being legally compliant and by providing secure products, services and solutions employing a secure development procedure.

The trust model established in clause 9 can be used to help determine trust-based security requirements for stakeholders.

10.2 Security requirements from trust level

10.2.1 Overview

The trust level in a stakeholder can be used to evaluate whether the stakeholder is able to provide an appropriate damage defence capability. Security requirements can be developed to mitigate such damage. As a result, security requirements can be based on organization capabilities including the professional level of the personnel, the use of secure development processes such as the security development lifecycle or security operation procedure capabilities and trustworthy solution related technology capabilities. For further details see standards and practices, such as [b-NIST FICIC], [b-BSIMM]. See Table 7.

Table 7 – Trust level and security requirement categories

Trust level	Security requirement categories		
Subject	Object		
	Organization capability (good credit)	System development and product lifecycle security or security operation capability (good procedure)	Trustworthiness solution related technology capability (good solution)
High	√	√	√
Medium	√	√	–
Low	√	–	–

10.2.2 Organization requirements

10.2.2.1 Introduction

The trust-related security capabilities of an organization can be broken down into: its reputation; its ability to execute contracts; the consistency of values; the possible compensation for breaches of contract; and its independence.

10.2.2.2 Reputation

Reputation reflects the degree of historical adherence to specified goals for a product or system. Reputation is a measurement that could be derived from direct or indirect knowledge of earlier interactions of stakeholders and is used to assess the level of trust in a stakeholder. As a representation of confidence, trust usually relies on historical information to infer the probability of future trustworthiness. Therefore, when a specific stakeholder has previously performed well in accordance with an agreement, its reputation in the industry will also be increased, and thus it can gain greater confidence from the other party. The data for the reputation management can be obtained from various reliable and widely accepted resources based on evidence, such as certificates or official annual and financial reports. However, a specific stakeholder may have different reputations in different fields. For example, the relationship between a device manufacturer and a network operator or service provider is that of vendor-customer, while that between different manufacturers may be competitive. Therefore, a device manufacturer can have a good reputation with a network operator or service provider, but a bad one with a competitor. As a result, when reviewing externally provided reputation information, network operators or service providers cannot take reputation information obtained from a competing manufacturer as a primary source.

10.2.2.3 Contract execution

In the case of cooperative execution that is continuous or multiple intermittent, the quality of the contract execution will have an impact on the confidence of both parties. It will also have an impact on the trust relationship between the parties. When the contract is executed well, mutual confidence will rise and the trust relationship will be tight. On the contrary, when the execution of the contract is not good, mutual confidence will decline, in addition to the trust relationship. For continuous multiple cooperation, for example, when visiting a service provider multiple times, the historical experience of users will directly impact their trust in the service system. In this case, the user's historical experience information is recommended for categorization as an issue concerned with the user's contract execution rather than reputation.

10.2.2.4 Consistency of valuee

When stakeholders share the same values, the relationship between them is closer and their expectations for the long-term future are more consistent. As a result, higher mutual confidence is achieved, and a better trust relationship will exist between them.

10.2.2.5 Compensation

Compensation capability relates to the expectation of compensation if a commitment is not upheld. An expectation of compensation can be regarded as another guarantee that the stakeholder seeks to perform the contract even in abnormal circumstances. In general, the more generous the compensation, the smaller loss on the peer is implied. Such a capability will increase confidence and trust in the other party. For example, regional cyber laws can dictate the level and severity of punishment or compensation for the various stakeholders to promote trustworthiness.

10.2.2.6 Independence

The independence of the stakeholder reflects its autonomy in executing the contract. Independence includes the ability of a parent company to control a subsidiary, and also includes the influence of authorities on the business entity. The more stakeholders it involves, the more influence it will receive from them and its trust relationship will be more affected.

10.2.2.7 Summary

An example of ways in which trust levels can relate to the capabilities of an organization is shown in Table 8. In practice, the precise choices for which aspects will be required for the medium and low trust levels vary depending on the application domain. For example, an appropriate supplier reputation may, in some cases, still be required to achieve a low trust level, whereas in other cases this aspect may not be significant even when a medium trust level is needed.

Table 8 – Trust levels and security requirements related to organization capabilities

Trust level	**Security requirements in organization capability aspect**				
	Reputation	**Contract execution**	**Consistency of value**	**Compensation capability**	**Independence**
High	✓	✓	✓	✓	✓
Medium	(✓)	✓	–	✓	(✓)
Low	–	✓	–	(✓)	–

10.2.3 Procedure requirements

10.2.3.1 Introduction

The security operation capability can be met by employing the following capabilities: Development and product lifecycle security; and security operation capability.

10.2.3.2 Development and product lifecycle security

Within the NESAS, the development and product lifecycle cover all aspects potentially impacting a network product's lifetime, including it being planned, designed, implemented, delivered, updated, and eventually ramped down. Currently, for the IMT-2020 network, NESAS, jointly developed by the Global System for Mobile Communications Association (GSMA) and the 3GPP, has determined a development and product lifecycle security towards IMT-2020 network equipment covering the stages through which network products pass throughout their development (including planning, design, implementation, testing, release, production and delivery) and product lifecycle (covering the stages through which developed network products proceed to end of life, including maintenance and update releases). It is recommended to take reference for vendor development and product lifecycle evaluation.

10.2.3.3 Security operation capability

Security operation capability means that the product or network needs to be well managed when commercially used, including security deployment, hardening and restricted access control.

10.2.3.4 Summary

So, with respect to the security operation capability, the security requirements listed in Table 9 are recommended.

Table 9 – Trust level and security requirements for security operation capability

Trust level	Security requirements for security operation capability	
	System development and product lifecycle security	Security operation
High	√	√
Medium	(√)	√
Low	=	√

10.2.4 Technology requirements

The trustworthiness capability can be met by meeting appropriate levels in the following respects: security procedures; privacy; resiliency; safety; reliability; and availability. These are the key attributes that the product and security solutions provided by the stakeholder are recommended to have from a trustworthiness point of view, as described in a range of documents such as [b-BSI 10754-1] and [b-NIST SP800-160v1].

An example of ways in which trust levels can be related to the trustworthiness of an organization is shown in Table 10. As previously, in practice, the precise choices for which aspects are required for the medium and low trust levels will vary depending on the application domain. For example, an appropriate level of data privacy protection may, in some cases, still be required to achieve a low trust level, whereas in other cases this aspect may not be significant even when a medium trust level is needed.

Table 10 – Trust level and security requirements for trustworthiness capability

Trust level	Security requirements for trustworthiness capability					
	Security procedure	Privacy	Resiliency	Safety	Reliability	Availability
High	√	√	√	√	√	√
Medium	√	(√)	(√)	(√)	(√)	√
Low	√	–	–	(√)	(√)	–

In real-world implementations, the precise requirements depend on service scenarios, and flexibility needs to be permitted. As previously noted, if the trust level is low, although the security requirements may be relatively low, there may be a need for a specific stronger requirement, such as privacy.

10.3 Interpreting trust to detailed assurance requirements

Once the required trust level has been determined for a particular use case, it is necessary to interpret this trust level to make implementation and operational decisions.

This can be achieved by mapping the required trust level to specific requirements listed in clause 10.2, and such requirements can be fulfilled through product and system assurance. There exists a range of long-established and standardized techniques for assuring the trustworthiness of products and systems through tests and evaluations, e.g., as carried out by specialist third parties. These can be used as the basis of a mapping from the required trust level, resulting from an analysis of the type described in clause 9.4, to the precise assurance requirements on equipment and service acquisition and use.

The example in Table 11 is intended to enable trust requirement levels to be mapped to trust-based business and operational decisions based on product and system evaluations.

Table 11 – Example mapping of required trust level to assurance requirements

Required trust level	Type of assurance entity	Security assurance scheme examples
High	Assessment by a recognized public body	Common criteria [b-ISO/IEC 15408 (all parts)] National regulatory body [b-ISO/IEC 27001] NESAS Security assurance specification (SCAS) [b-3GPP TS33.511] [b-3GPP TS33.512] [b-3GPP TS33.513] [b-3GPP TS33.514] [b-3GPP TS33.515] [b-3GPP TS33.516] [b-3GPP TS33.517] [b-3GPP TS33.518] [b-3GPP TS33.519]
Medium	Evaluation by an accredited conformity assessment body (CAB)	Common criteria [b-ISA/IEC 62443 (all parts)] [b-ISO/IEC 27001] NESAS/SCAS
Low	Evaluation by a CAB or self-assessment	Common criteria NESAS/SCAS

Even within a particular assurance scheme, different degrees or types of assurance guarantees may be appropriate for different trust levels.

- Some techniques, notably as specified in [b-ISO/IEC 15408 (all parts)], allow multiple levels of assurance to be specified, so that different trust levels can optionally require different levels of [b-ISO/IEC 15408 (all parts)] evaluation. However, other schemes, such as [b-ISO/IEC 27001], allow only a single level of evaluation.
- The degree of assurance obtainable from an evaluation can optionally vary depending on the body performing it (as indicated by the middle column in Table 11). For example, self-evaluation against the requirements of [b-ISO/IEC 27001] might be appropriate for the low trust level.

Moreover, the weight given to an evaluation can be reinforced by other factors, for example:

- whether the equipment or service is critical for mission delivery or is just one of multiple ways in which a particular function can be provided (e.g., through redundancy);
- whether there are multiple assurance evaluations relating to different aspects of a particular product, system or service.

Bibliography

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers*.

[b-ISO 28598-1] ISO 28598-1:2017, *Acceptance sampling procedures based on the allocation of priorities principle (APP) – Part 1: Guidelines for the APP approach*.

[b-ISO 31000] ISO 31000:2018, *Risk management – Guidelines*. Available [viewed 2022-07-18] at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en .

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary*.

[b-ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.

[b-ISO/IEC/IEEE 15288] ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*.

[b-ISO/IEC 15408(all parts)] ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security*

[b-ISO/IEC/IEEE 24765] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*.

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27005] ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management*.

[b-ISO/PAS 19450] Publicly Available Specification ISO/PAS 19450:2015, *Automation systems and integration – Object-process methodology*.

[b-ISO/TS 21089] Technical Specification ISO/TS 21089:2018, *Health informatics – Trusted end-to-end information flows.*

[b-ISO/TS 21719-2] Technical Specification ISO/TS 21719-2:2018, *Electronic fee collection – Personalization of on-board equipment (OBE) Part 2: Using dedicated short-range communication*.

[b-ISO/TS 22318] Technical Specification ISO/TS 22318:2021, *Security and resilience – Business continuity management systems – Guidelines for supply chain continuity management*.

[b-ISA/IEC 62443] ISA/IEC 62443 (all parts) [series of automation and control systems cybersecurity standards].

[b-GSMA FS.13] GSM Association (2022). *Network equipment security assurance scheme – Overview*, Official Document FS.13, version 2.1. London: GSM Association. 29 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf

[b-GSMA FS.14] GSM Association (2022). *Network equipment security assurance scheme –Security test laboratory accreditation*, Official Document FS.14, version 2.1. London: GSM Association. 15 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.14-v2.1.pdf .

[b-GSMA FS.15] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle assessment methodology*, Official Document FS.15, version 2.1. London: GSM Association. 33 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.15-v2.1.pdf .

[b-GSMA FS.16] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle security requirements*, Official Document FS.16, version 2.1. London: GSM Association. 22 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf .

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol – Version 1.2*.

[b-IETF RFC 6733] IETF RFC 6733 (2012), *Diameter base protocol*.

[b-3GPP TS 33.501] Technical Specification 3GPP TS 33.501 V17.6.0 (2022), *Security architecture and procedures for 5G system*.

[b-3GPP TS 33.511] Technical Specification 3GPP TS 33.511 V17.1.0 (2022), *Security assurance specification (SCAS) for the next generation node B (gNodeB) network product class*.

[b-3GPP TS 33.512] Technical Specification 3GPP TS 33.512 V17.3.0 (2022), *5G security assurance specification (SCAS); Access and mobility management function (AMF)*.

[b-3GPP TS 33.513] Technical Specification 3GPP TS 33.513 V17.0.0 (2022), *5G security assurance specification (SCAS); User plane function (UPF)*.

[b-3GPP TS 33.514] Technical Specification 3GPP TS 33.514 V17.0.0 (2022), *5G security assurance specification (SCAS) for the unified data management (UDM) network product class*.

[b-3GPP TS 33.515] Technical Specification 3GPP TS33.515 V17.0.0 (2022), *5G security assurance specification (SCAS) for the session management function (SMF) network product class*.

[b-3GPP TS 33.516] Technical Specification 3PGP TS33.516 V17.0.0 (2022), *5G security assurance specification (SCAS) for the authentication server function (AUSF) network product class*.

[b-3GPP TS 33.517] Technical Specification 3GPP TS33.517 V17.0.0 (2022), *5G security assurance specification (SCAS) for the security edge protection proxy (SEPP) network product class*.

[b-3GPP TS 33.518] Technical Specification 3GPP TS33.518 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network repository function (NRF) network product class*.

[b-3GPP TS 33.519] Technical Specification 3GPP TS33.519 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network exposure function (NEF) network product class*.

[b-BSI 10754-1] BS 10754-1:2018, *Information technology. Systems trustworthiness – Governance and management specification*.

[b-BSIMM] British Standards Institution (2021). *Building security in maturity model,* BSIMM 12. London: British Standards Institution.

[b-NIST FICIC] NIST (2018). *Framework for improving critical infrastructure cybersecurity,* Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. 48 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[b-NIST SP800-30] Joint Task Force Transformation Initiative (2012). *Guide for conducting risk assessments,* NIST Special Publication, NIST SP800-30 Rev.1. Gaithersburg, MD: National Institute of Standards and Technology. 95 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf .

[b-NIST SP 800-53] NIST SP 800-53 Rev 5 2020, *Security and privacy controls for information systems and organizations*.

[b-NIST SP800-160v1] Ross, R., McEvilley, M., Carrier Oren, J. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems – Volume 1,* NIST Special Publication, NIST SP800-160v1. Gaithersburg, MD: National Institute of Standards and Technology. 243 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf .

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022